On the Existence of Optimum Cyclic Burst-Correcting Codes

KHALED A. S. ABDEL-GHAFFAR, ROBERT J. McELIECE, FELLOW, IEEE, ANDREW M. ODLYZKO, MEMBER, IEEE, AND HENK C. A. VAN TILBORG, SENIOR MEMBER, IEEE

Abstract—**It is shown that for each integer $b \geq 1$ infinitely many optimum cyclic b-burst-correcting codes exist, i.e., codes whose length n, redundancy r, and burst-correcting capability b, satisfy $n = 2^{r-b+1} - 1$. Some optimum codes for $b = 3$, 4, and 5 are also studied in detail.**

I. INTRODUCTION

IN THIS PAPER, a binary code is called a *b-burst-correcting code* if it can correct any single cyclic burst of length b, or less. If C is an $[n, n-r]$ b-burst-correcting code, then the syndromes corresponding to the different cyclic bursts of lengths $\leq b$ should be nonzero and distinct. Since there are $n2^{b-1}$ different cyclic bursts of length up to b, it follows that $2^r \geq 1 + n2^{b-1}$. Abramson [1] noted that this inequality, along with the fact that n is an integer, implies

$$n \leq 2^{r-b+1} - 1. \tag{1.1}$$

A b-burst-correcting code which satisfies (1.1) with equality is said to be *optimum*. In this paper we will show that for every value of b, an infinite number of optimum cyclic codes exists. From (1.1) it follows that an optimum code has length $n = 2^m - 1$, where $m = r - b + 1$. The Rieger inequality $r \geq 2b$ [2], which holds for linear b-burst-correcting codes containing more than one codeword, implies that $m \geq b + 1$.

From now on, we will consider only optimum cyclic codes. It is well-known that if $p(x)$ is a primitive polynomial of degree m, then it generates an optimum one-burst-correcting code, which is simply a Hamming code. Abramson [3] has proved that $(1 + x)p(x)$, where $p(x)$ is a primitive polynomial of degree $m \geq 3$, generates an optimum two-burst-correcting code. In [1], Abramson noted that $(1 + x + x^2)p(x)$, where $p(x)$ is a primitive polynomial of even degree $m \geq 4$ satisfying $1 + x \equiv x^a \pmod{p(x)}$ for $a \not\equiv 2 \pmod 3$, generates an optimum three-burst-correcting code. He exhibited such codes for $m = 4, 6, 8, 10$ and conjectured that they exist for every even $m \geq 4$.

Elspas and Short [4] have stated necessary conditions on the generator polynomials of optimum burst-correcting codes. These conditions are stated in Theorem 1. First we need the following definition. Let $e(x)$ be a polynomial over F_2 of positive degree. Let m_e be the least common multiple (LCM) of the degrees of the irreducible factors of $e(x)$ over F_2. Obviously, 2^{m_e} is the order of the splitting field of $e(x)$. We say that m_e is the *degree of the splitting field of* $e(x)$. If $e(x) = 1$, we define $m_e = 1$.

Theorem 1: If a polynomial $g(x)$ generates an optimum b-burst-correcting code, then it can be factored as $e(x)p(x)$, where $e(x)$ and $p(x)$ satisfy the following conditions:

1) the polynomial $e(x)$ is a square-free polynomial of degree $b - 1$ which is not divisible by x;
2) the polynomial $p(x)$ is a primitive polynomial of degree $m \geq b + 1$ such that $m \equiv 0 \pmod{m_e}$, where m_e is the degree of the splitting field of $e(x)$.

Since the proof of this theorem, which plays a central role in the present paper, is omitted in [4], we prove it in Appendix I.

Elspas and Short [4] have also studied four-burst-correcting codes generated by $(1 + x^3)p(x)$, where $p(x)$ is a primitive polynomial of even degree $m \geq 6$. They found that no such code exists for $m < 10$ and that for $m = 10$ there exist ten codes while for $m = 12$ there are 26 codes.[1] Elspas and Short also studied four-burst-correcting codes generated by $(1 + x + x^3)p(x)$, where $p(x)$ is a primitive polynomial of degree m such that $3|m$ and $m \geq 6$. They reported that no such code exists for $m < 9$, and that they exist for $m = 9$, 12. No optimum b-burst-correcting code has been reported in the literature for $b > 4$.

Manuscript received August 28, 1985; revised January 27, 1986. This work was supported in part by the Defense Advanced Research Projects Agency under ARPA order 3771 and in part by the Office of Naval Research under Contract N00014-79-C-0597. This paper was presented at the IEEE International Symposium on Information Theory, Ann Arbor, MI, October 1986.

K. A. S. Abdel-Ghaffar and R. J. McEliece are with the Department of Electrical Engineering, California Institute of Technology, Pasadena, CA 91125.

A. M. Odlyzko is with Bell Laboratories, Murray Hill, NJ 07974.

H. C. A. van Tilborg is with the Department of Mathematics and Computing Science, Eindhoven University at Technology, 5600 MB, Eindhoven, The Netherlands.

IEEE Log Number 8609499.

[1] Unfortunately, typographical errors occurred in two of the generator polynomials reported for $m = 10$, namely, (01) (012) (0234,10) and (01) (012)(0123458,10). The polynomials (0234,10) and (0123458,10) are not primitive and thus violate Condition 2 of Theorem 1. These polynomials should be replaced by (0235,10) and (023458,10). The first erroneous generator polynomial is found in numerous tables of burst-correcting codes reported in the literature, e.g., [5, p. 373], [6, p. 364], [7, p. 271], [8, p. 115].

0018-9448/86/1100-0768$01.00 ©1986 IEEE

In this paper, we will show that for every b, for every polynomial $e(x)$ subject to condition 1 of Theorem 1, and for every sufficiently large $m \equiv 0 \pmod{m_e}$, a primitive polynomial $p(x)$ of degree m exists such that $e(x)p(x)$ generates an optimum b-burst-correcting code of length $2^m - 1$. First, in Section II, we will derive conditions on the primitive polynomial $p(x)$ which ensure that $e(x)p(x)$ generates an optimum b-burst-correcting code. Then, in Section III, we will argue using some results from algebraic geometry, namely, Weil's estimates for character sums, that for sufficiently large $m \equiv 0 \pmod{m_e}$, polynomials $p(x)$ of degree m exist satisfying the conditions stated in Section II.

The conjecture of Abramson that, for every even $m \geq 4$ there exists an optimum three-burst-correcting code of length $2^m - 1$, is proved in Section IV. We also prove, in Section V, that for every even $m \geq 10$ an optimum four-burst-correcting code of length $2^m - 1$ exists. Finally, in Section VI, we give an explicit example of an optimum five-burst-correcting code of length $2^{15} - 1$.

II. Sufficient Conditions for Optimum Cyclic Burst-Correcting Codes

Let C be an $[n, n-r]$ binary linear code. A *cyclic burst* of length b, $b \geq 1$, is a binary n-tuple, $(v_i)_{0 \leq i < n}$, whose nonzero components, considered cyclically, are confined to a string of length b, but not smaller. In other words, $(v_i)_{0 \leq i < n}$ is a burst of length b if for some integer l, $0 \leq l < n$, $v_l = v_{l+b-1} = 1$ and $v_i = 0$ for $i \notin \{l, l+1, \cdots, l+b-1\}$ where all integers are considered modulo n. The burst $(v_i)_{0 \leq i < n}$ can be represented as $x^l B(x) \bmod x^n + 1$, where $B(x) = \sum_{i=0}^{b-1} v_{l+i} x^i$.

Let

$$\mathscr{B}_b = \{ f(x) \in F_2[x] : \deg f(x) < b, f(0) \neq 0 \}. \quad (2.1)$$

Then $x^l B(x) \bmod x^n + 1$, where $0 \leq l < n$, represents a burst of length $\leq b$, if and only if $B(x) \in \mathscr{B}_b$.

The following lemma gives necessary and sufficient conditions for a cyclic code generated by $e(x)p(x)$, where $e(x)$ and $p(x)$ satisfy conditions 1 and 2 of Theorem 1, to be a b-burst-correcting code. We define $\mathscr{B}_b^* = \mathscr{B}_b - \{e(x)\}$.

Lemma 1: Let $e(x)$ and $p(x)$ satisfy conditions 1 and 2 of Theorem 1. Then $e(x)p(x)$ generates a b-burst-correcting code which is optimum and of length $2^m - 1$ if and only if for $0 \leq l < 2^m - 1$ and for all distinct polynomials $B_1(x), B_2(x) \in \mathscr{B}_b^*$, $B_1(x) + x^l B_2(x) \equiv 0 \pmod{e(x)}$ implies $B_1(x) + x^l B_2(x) \not\equiv 0 \pmod{p(x)}$.

Proof: In general, a linear code is a b-burst-correcting code if and only if no codeword except the all-zero codeword is the sum of two cyclic bursts of length b or less. Hence $e(x)p(x)$ generates a b-burst-correcting code if and only if, for $0 \leq l < n$ and for all polynomials $B_1(x)$ and $B_2(x)$ whose degrees are less than b,

$$B_1(x) + x^l B_2(x) \equiv 0 \pmod{e(x)p(x)} \quad (2.2)$$

implies $B_1(x) + x^l B_2(x) = 0$. This lemma says that this condition is satisfied if (2.2) does not hold for $0 \leq l < 2^m - 1$ and for all distinct polynomials $B_1(x), B_2(x) \in \mathscr{B}_b^*$. Thus it remains to prove that $B_1(x) = x^l B_2(x)$ if (2.2) holds with $B_1(x) = B_2(x)$, or if at least one of the polynomials $B_1(x)$ or $B_2(x)$ is zero or equal to $e(x)$. Suppose that (2.2) holds with $B_1(x) = B_2(x) \neq 0$. Then $p(x) | 1 + x^l$, which implies $2^m - 1 | l$, and hence $l = 0$. Secondly, if $B_1(x)$ or $B_2(x)$ is zero, then clearly the other one is also zero. Finally, suppose that (2.2) holds with $B_1(x)$ or $B_2(x)$ equal to $e(x)$ and none of them is zero. Then $e(x) | B_1(x) + x^l B_2(x)$ implies that $B_1(x) = B_2(x) = e(x)$, and $l = 0$. ∎

Next, we will give a different form for the necessary and sufficient condition of Lemma 1. First, we need some more notation. Let h be the period of $e(x)$. Then $h | 2^m - 1$, the length of the code. For each $B(x) \in \mathscr{B}_b^*$ define the integer $a(B)$ uniquely by

$$B(x) \equiv x^{a(B)} \pmod{p(x)}, \qquad 0 \leq a(B) < 2^m - 1.$$

The integer $a(B)$ is called the *index* of $B(x)$.

The condition $B_1(x) + x^l B_2(x) \not\equiv 0 \pmod{p(x)}$ can then be stated as $a(B_1) - a(B_2) \not\equiv l \pmod{2^m - 1}$. Hence the necessary and sufficient condition stated in Lemma 1 is equivalent to a set of conditions of the form $a(B_1) - a(B_2) \not\equiv l \pmod{2^m - 1}$, where $0 \leq l < 2^m - 1$ and $B_1(x), B_2(x) \in \mathscr{B}_b^*$ are distinct polynomials such that $B_1(x) + x^l B_2(x) \equiv 0 \pmod{e(x)}$. However, if $B_1(x) + x^l B_2(x) \equiv 0 \pmod{e(x)}$, then $B_1(x) + x^{l'} B_2(x) \equiv 0 \pmod{e(x)}$ for all $l' \equiv l \pmod{h}$. Thus the conditions can be written in the form $a(B_1) - a(B_2) \not\equiv l \pmod{h}$, where $0 \leq l < h$, and $B_1(x), B_2(x)$ as described before.

Although this is not yet the final form we shall obtain for the necessary and sufficient condition stated in Lemma 1, let us study a specific example.

Example

Let $b = 4$, and $e(x) = 1 + x^3 = (1+x)(1+x+x^2)$. Clearly, $e(x)$ satisfies condition 1. Now let $p(x)$ be a primitive polynomial of even degree $m \geq 6$. Then $p(x)$ satisfies condition 2. In this example, $h = 3$ and $\mathscr{B}_b^* = \{1, 1+x, 1+x^2, 1+x+x^2, 1+x+x^3, 1+x^2+x^3, 1+x+x^2+x^3\}$. We consider the 21 different pairs of distinct polynomials $B_1(x), B_2(x) \in \mathscr{B}_b^*$, and for each pair we look for all values of $l, 0 \leq l < 3$, such that $B_1(x) + x^l B_2(x) \equiv 0 \pmod{1+x^3}$. For each value of l satisfying this congruency, $p(x)$ must satisfy $a(B_1) - a(B_2) \not\equiv l \pmod 3$. For example, let $B_1(x) = 1$ and $B_2(x) = 1 + x$. Then $1 + x^l(1+x) \not\equiv 0 \pmod{1+x^3}$ for $l = 0, 1, 2$. Hence no condition is imposed on $p(x)$ by the pair $(1, 1+x)$. In fact, the only pairs which impose conditions on $p(x)$ are $(1, 1+x+x^3)$, $(1, 1+x^2+x^3)$, $(1+x, 1+x^2)$, $(1+x, 1+x+x^2+x^3)$, $(1+x^2, 1+x+x^2+x^3)$, $(1+x+x^3, 1+x^2+x^3)$. For example, for the pair $(1, 1+x+x^3)$, we have $1 + x^l(1+x+x^3) \equiv 0 \pmod{1+x^3}$ for $0 \leq l < 3$, if and only if $l = 2$. Hence this pair imposes the condition $a(1) - a(1+x+x^3) \not\equiv 2 \pmod 3$. Studying the six pairs, the following six conditions can be

deduced:

1) $a(1) - a(1 + x + x^3) \not\equiv 2 \pmod 3$,
2) $a(1) - a(1 + x^2 + x^3) \not\equiv 1 \pmod 3$,
3) $a(1 + x) - a(1 + x^2) \not\equiv 1 \pmod 3$,
4) $a(1 + x) - a(1 + x + x^2 + x^3) \not\equiv 2 \pmod 3$,
5) $a(1 + x^2) - a(1 + x + x^2 + x^3) \not\equiv 1 \pmod 3$,
6) $a(1 + x + x^3) - a(1 + x^2 + x^3) \not\equiv 2 \pmod 3$.

These conditions on $p(x)$ can be further simplified. For this we define $\mathscr{F}_b$ to be the set of all irreducible polynomials of degrees less than b and not including x, i.e.,

$$\mathscr{F}_b = \{ f(x) \in \mathscr{B}_b : f(x) \text{ is irreducible} \}. \quad (2.3)$$

From the unique factorization theorem, it follows that any polynomial $B(x) \in \mathscr{B}_b$ of positive degree, i.e., $B(x) \neq 1$, can be factored uniquely as

$$B(x) = f_1(x) f_2(x) \cdots f_k(x), \quad \text{where } f_i(x) \in \mathscr{F}_b \text{ for } 1 \leq i \leq k.$$

Hence

$$a(B) \equiv a(f_1) + a(f_2) + \cdots + a(f_k) \pmod{2^m - 1}. \quad (2.4)$$

We also have $a(1) = 0$. Hence the conditions on $p(x)$ can be written in the form

$$\sum_{f \in \mathscr{F}_b} \lambda_f a(f) \not\equiv l \pmod h$$

for some values of λ_f, $0 \leq \lambda_f \leq h - 1$. The set of conditions $a(B_1) - a(B_2) \not\equiv l \pmod h$ for $0 \leq l < h$, and for all pairs of distinct polynomials $B_1(x), B_2(x) \in \mathscr{B}_b^*$ such that $B_1(x) + x^l B_2(x) \equiv 0 \pmod{e(x)}$, and where $a(B_1)$, $a(B_2)$ are expressed in terms of $a(f)$ for $f(x) \in \mathscr{F}_b$ as in (2.4), will be called the *Abramson–Elspas–Short (AES) conditions* associated with $e(x)$. From this formulation of the condition stated in Lemma 1, we get the following theorem.

Theorem 2: A polynomial $g(x)$ generates an optimum b-burst-correcting code if and only if it can be factored as $e(x)p(x)$, where

1) the polynomial $e(x)$ is a square-free polynomial of degree $b - 1$ which is not divisible by x;
2) the polynomial $p(x)$ is a primitive polynomial of degree $m \geq b + 1$ such that $m \equiv 0 \pmod{m_e}$, where m_e is the degree of the splitting field of $e(x)$;
3) the polynomial $p(x)$ satisfies the AES conditions associated with $e(x)$.

Now, let us return to the example and find the AES conditions associated with $1 + x^3$.

Example (Continued): We have $\mathscr{F}_4 = \{1 + x, 1 + x + x^2, 1 + x + x^3, 1 + x^2 + x^3\}$. As in (2.4), $a(1 + x^2) = 2a(1 + x)$ and $a(1 + x + x^2 + x^3) = 3a(1 + x)$. We also have $a(1) = 0$. Substituting this in the six conditions derived earlier and using the simpler notation $a_1 = a(1 + x)$, $a_2 = a(1 + x + x^3)$, $a_3 = a(1 + x^2 + x^3)$, we get the following four conditions modulo 3:

1) $a_1 \not\equiv 2$,
2) $a_2 \not\equiv 1$,
3) $a_3 \not\equiv 2$,
4) $a_2 + 2a_3 \not\equiv 2$.

These are the AES conditions associated with $1 + x^3$. They have the following solutions:

$a_1 \bmod 3$	$a_2 \bmod 3$	$a_3 \bmod 3$
0	0	0
1	0	0
0	2	1
1	2	1

If $b = 1$, then $e(x) = 1$. In this case the set $\mathscr{B}_b^*$ is empty, and hence no AES conditions are imposed on $p(x)$. (Of course, this is not the shortest proof that Hamming codes are single-error-correcting codes!) In case $b = 2$, $e(x) = 1 + x$, and the set $\mathscr{B}_b^*$ contains only one polynomial, which is one. Again, this means that no AES conditions are imposed on $p(x)$. Hence $(1 + x)p(x)$, where $p(x)$ is a primitive polynomial of degree $m \geq 3$, generates an optimum two-burst-correcting code of length $2^m - 1$. Such codes are known as Abramson codes [3]. We have nothing more to say about the cases $b = 1$ or 2. In the rest of this paper we consider $b \geq 3$.

Obviously, it is necessary to know whether the AES conditions associated with a polynomial $e(x)$ satisfying condition 1 have solutions. In the example, we note that $a(f) \equiv 0 \pmod 3$ for all $f(x) \in \mathscr{F}_4$ is a solution of the AES conditions associated with $1 + x^3$. The next theorem gives a generalization of this result.

Theorem 3: Let $e(x)$ be a square-free polynomial of degree $b - 1$ which is not divisible by x. Let h be its period. Then $a(f) \equiv 0 \pmod h$ for $f(x) \in \mathscr{F}_b$ is a solution of the AES conditions associated with $e(x)$.

Proof: Suppose, to get a contradiction, that $a(f) \equiv 0 \pmod h$ for $f(x) \in \mathscr{F}_b$ is not a solution of the AES conditions. Then, there exist an integer l, $0 \leq l < h$ and two distinct polynomials $B_1(x), B_2(x) \in \mathscr{B}_b^*$ such that $B_1(x) + x^l B_2(x) \equiv 0 \pmod{e(x)}$ and $a(B_1) - a(B_2) \equiv l \pmod h$. However, if $a(f) \equiv 0 \pmod h$ for $f(x) \in \mathscr{F}_b$, then, from (2.4), it follows that $a(B) \equiv 0 \pmod h$ for all $B(x) \in \mathscr{B}_b^*$ and in particular for $B_1(x)$ and $B_2(x)$. Hence $l = 0$ and $B_1(x) + B_2(x) \equiv 0 \pmod{e(x)}$. Since $B_1(x)$ and $B_2(x)$ are distinct and of degree $\leq b - 1$, it follows that $B_1(x) + B_2(x) = e(x)$. This contradicts $B_1(0) = B_2(0) = e(0) = 1$, which follows from definition (2.1) and the hypotheses of the theorem. ■

III. The Existence of Optimum Cyclic Burst-Correcting Codes

In this section, the most important result of this paper is proved. Let $e(x)$ be a polynomial which satisfies condition 1. We will prove that, for all sufficiently large m subject to

condition 2, a primitive polynomial $p(x)$ of degree m exists which satisfies condition 3. For such $p(x)$, the polynomial $e(x)p(x)$ generates an optimum cyclic b-burst-correcting code of length $2^m - 1$.

This result looks very plausible. There are $\phi(2^m - 1)/m$ primitive polynomials of degree m, where ϕ is Euler's function. Hence, for large m, the number of primitive polynomials of degree m becomes very large, and one should be able to find a *good* polynomial among them. Unfortunately, to make this argument rigorous, we need advanced mathematical tools. In this section, we use Weil's estimates of character sums with polynomial arguments as presented in, e.g., [9, ch. 5], [10, ch. II].

Let $b \geq 3$, and let $e(x)$ be a polynomial which satisfies condition 1. Let h be the period of $e(x)$, and let m_e the degree of its splitting field. It follows that $h \geq 3$. Let m be an integer, $m \geq b + 1$, such that $m \equiv 0 \pmod{m_e}$. A multiplicative character of $\boldsymbol{F}_q$, where $q = 2^m$, is denoted by χ. A character χ of order j is denoted by χ_j. In particular, χ_1 is the trivial character. By definition, $\chi(0) = 0$. As usual, $\boldsymbol{F}_q^*$ denotes the multiplicative group of $\boldsymbol{F}_q$. The following lemma can easily be proved.

Lemma 2: Let z be an indeterminate, and let $\xi \in \boldsymbol{C}$ be a primitive hth root of unity. Then

$$\prod_{j=1}^{h-1} (1 - z\xi^j) = \sum_{j=0}^{h-1} z^j.$$

A proof of the following lemma appears in [11].

Lemma 3: Let

$$\psi(\alpha) = \sum_{k \mid q-1} \frac{\mu(k)}{k} \sum_{\chi^k = \chi_1} \chi(\alpha) \tag{3.1}$$

where $\alpha \in \boldsymbol{F}_q^*$ and μ is the Möbius function. Then

$$\psi(\alpha) = \begin{cases} 1, & \text{if } \alpha \text{ is primitive,} \\ 0, & \text{otherwise.} \end{cases}$$

In the following, $\mathscr{F} = \{f_1(x), \cdots, f_M(x)\}$ is a nonempty subset of the set $\mathscr{F}_b$, which is defined in (2.3).

Lemma 4: Let

$$\theta(\alpha) = \psi(\alpha) \prod_{i=1}^{M} \sum_{j=0}^{h-1} \chi_h^j\left(\alpha^{-l_i} f_i(\alpha)\right) \tag{3.2}$$

where $\alpha \in \boldsymbol{F}_q^*$, $\psi(\alpha)$ is as defined in (3.1), and the l_i's are integers. Then

$$\theta(\alpha) = \begin{cases} h^M, & \text{if } \alpha \text{ is primitive and for all} \\ & 1 \leq i \leq M,\ a_i \equiv l_i \pmod{h}, \\ & \text{where } f_i(\alpha) = \alpha^{a_i},\ 0 \leq a_i < 2^m - 1, \\ 0, & \text{otherwise.} \end{cases}$$

Proof: From Lemma 3, it follows that $\theta(\alpha) = 0$ if α is not primitive. So let α be primitive, and apply Lemma 2 with $z = \chi_h(\alpha^{-l_i} f_i(\alpha)) = \chi_h(\alpha^{a_i - l_i})$ to get

$$\theta(\alpha) = \prod_{i=1}^{M} \prod_{j=1}^{h-1} \left(1 - \xi^j \chi_h(\alpha^{a_i - l_i})\right)$$

where $\xi \in \boldsymbol{C}$ is a primitive hth root of unity. The proof is obvious from the above form. ∎

In the next lemma, Weil's estimates are used. First, we state them.

Weil's Estimates [9, p. 225]: Let χ be a multiplicative character of order $j > 1$, and let $f \in \boldsymbol{F}_q[x]$ be a polynomial which is not a jth power of a polynomial. Let s be the number of distinct roots of f in its splitting field over $\boldsymbol{F}_q$. Then we have

$$\left| \sum_{\alpha \in \boldsymbol{F}_q} \chi(f(\alpha)) \right| \leq (s - 1) q^{1/2}.$$

In the following lemma, we need to estimate character sums over $\boldsymbol{F}_q^*$ rather than $\boldsymbol{F}_q$. Write $f(x) = x^L w(x)$ for nonnegative integer L such that $w(0) \neq 0$. Suppose that $w(x)$ is a polynomial of positive degree that is not a jth power of a polynomial. Let s' denote the number of distinct roots of $w(x)$ in its splitting field over $\boldsymbol{F}_q$. If $L = 0$, then

$$\begin{aligned} \left| \sum_{\alpha \in \boldsymbol{F}_q^*} \chi((f(\alpha)) \right| &\leq \left| \sum_{\alpha \in \boldsymbol{F}_q} \chi((f(\alpha)) \right| + 1 \\ &\leq (s' - 1) q^{1/2} + 1 \leq s' q^{1/2}. \end{aligned}$$

On the other hand, if $L \neq 0$, then $\chi(f(0)) = 0$, and we get

$$\left| \sum_{\alpha \in \boldsymbol{F}_q^*} \chi((f(\alpha)) \right| = \left| \sum_{\alpha \in \boldsymbol{F}_q} \chi((f(\alpha)) \right| \leq s' q^{1/2},$$

since $f(x)$ has in this case $s' + 1$ distinct roots. Thus, in both cases, we get

$$\left| \sum_{\alpha \in \boldsymbol{F}_q^*} \chi((f(\alpha)) \right| \leq s' q^{1/2}. \tag{3.3}$$

Lemma 5:

$$\left| \sum_{\alpha \in \boldsymbol{F}_q^*} \theta(\alpha) - \phi(q - 1) \right| \leq A(h, \mathscr{F}) q^{1/2} d(q - 1)$$

where $\theta(\alpha)$ is as defined in Lemma 4, d is the divisor function, and $A(h, \mathscr{F}) = (h - 1)h^{M-1} \sum_{t=1}^{M} \deg f_t$.

Proof: From (3.2), we have $\theta(\alpha) = \psi(\alpha) + R(\alpha)$, where

$$\begin{aligned} R(\alpha) = \psi(\alpha) \underbrace{\sum_{i_1=0}^{h-1} \cdots \sum_{i_M=0}^{h-1}}_{(i_1, \cdots, i_M) \neq (0, \cdots, 0)} & \chi_h^{i_1}\left(\alpha^{-l_1} f_1(\alpha)\right) \\ & \cdots \chi_h^{i_M}\left(\alpha^{-l_M} f_M(\alpha)\right). \end{aligned} \tag{3.4}$$

Summing over all $\alpha \in \boldsymbol{F}_q^*$, and using Lemma 3, we get

$$\sum_{\alpha \in \boldsymbol{F}_q^*} \theta(\alpha) = \phi(q - 1) + \sum_{\alpha \in \boldsymbol{F}_q^*} R(\alpha).$$

Hence, the proof of the lemma depends on showing that

$$\left| \sum_{\alpha \in \boldsymbol{F}_q^*} R(\alpha) \right| \leq (h - 1) h^{M-1} \sum_{t=1}^{M} (\deg f_t) q^{1/2} d(q - 1). \tag{3.5}$$

From (3.1), we have, by considering a typical term in the sum of the right side of (3.4),

$$\psi(\alpha)\chi_h^{i_1}(\alpha^{-l_1}f_1(\alpha))\cdots\chi_h^{i_M}(\alpha^{-l_M}f_M(\alpha)) = \sum_{k|q-1}\frac{\mu(k)}{k}\sum_{\chi^k=\chi_1}\chi(\alpha)\chi_h^{i_1}(\alpha^{-l_1}f_1(\alpha)) \cdots\cdots \chi_h^{i_M}(\alpha^{-l_M}f_M(\alpha)). \tag{3.6}$$

In the inner sum, $\chi = \chi_j$ for some $j|k$. Hence

$$\chi_j(\alpha)\chi_h^{i_1}(\alpha^{-l_1}f_1(\alpha))\cdots\chi_h^{i_M}(\alpha^{-l_M}f_M(\alpha)) = \chi_{q-1}(\alpha^L w(\alpha))$$

where

$$L = (q-1)\left(\frac{1}{j} - \frac{1}{h}(l_1 + \cdots + l_M)\right)$$

and

$$w(x) = \prod_{t=1}^{M}(f_t(x))^{(q-1)i_t/h}.$$

The polynomial $w(x)$ is a polynomial of positive degree which is not a $(q-1)$st power of a polynomial since $(i_1,\cdots,i_M) \neq (0,\cdots,0)$ and $0 \le i_t \le h-1$ for $1 \le t \le M$. The number of distinct roots of $w(x)$ in its splitting field is $\sum_{t=1}^{M} u(i_t)\deg f_t$, where $u(i)$ is defined over the nonnegative integers as $u(0) = 0$ and $u(i) = 1$ for $i \ge 1$. Hence from (3.3), we get

$$\left|\sum_{\alpha\in F_q^*}\chi_j(\alpha)\chi_h^{i_1}(\alpha^{-l_1}f_1(\alpha))\cdots\chi_h^{i_M}(\alpha^{-l_M}f_M(\alpha))\right| \le \sum_{t=1}^{M}u(i_t)(\deg f_t)q^{1/2}.$$

Using (3.6) and noting that there are exactly k characters χ such that $\chi^k = \chi_1$, we get

$$\left|\sum_{\alpha\in F_q^*}\psi(\alpha)\chi_h^{i_1}(\alpha^{-l_1}f_1(\alpha))\cdots\chi_h^{i_M}(\alpha^{-l_M}f_M(\alpha))\right| \le \sum_{t=1}^{M}u(i_t)(\deg f_t)q^{1/2}d(q-1).$$

Using (3.4) along with the foregoing inequality, we get

$$\left|\sum_{\alpha\in F_q^*}R(\alpha)\right| \le \underbrace{\sum_{i_1=0}^{h-1}\cdots\sum_{i_M=0}^{h-1}}_{(i_1,\cdots,i_M)\neq(0,\cdots,0)}\sum_{t=1}^{M}u(i_t)\cdot(\deg f_t)q^{1/2}d(q-1) = \sum_{t=1}^{M}h^{M-1}\sum_{i_t=1}^{h-1}u(i_t)(\deg f_t)q^{1/2}d(q-1)$$

where we have interchanged the order of summation. Since $u(i) = 1$ for $i > 1$, (3.5) is proved. ■

From Lemma 4, $\sum_{\alpha\in F_q^*}\theta(\alpha)$ is h^M times the number of primitive elements α such that $a_i \equiv l_i \pmod h$, where $f_i(\alpha) = \alpha^{a_i}$ for $1 \le i \le M$. Hence if $\sum_{\alpha\in F_q^*}\theta(\alpha) > 0$, then such a primitive element exists, and its minimal polynomial over F_2 is a primitive polynomial, $p(x)$, of degree m that satisfies $a_i \equiv l_i \pmod h$, where $f_i(x) \equiv x^{a_i} \pmod{p(x)}$ for $1 \le i \le M$. From Lemma 5, it follows that if $\phi(q-1) - A(h,\mathcal{F})q^{1/2}d(q-1) > 0$, then $\sum_{\alpha\in F_q^*}\theta(\alpha) > 0$. However, from [12, pp. 260–267], we have for any given $\epsilon > 0$, $d(q-1) < q^{\epsilon}$ and $\phi(q-1) > q^{1-\epsilon}$ for sufficiently large q. Since $A(h,\mathcal{F})$ does not depend on q, $\phi(q-1) - A(h,\mathcal{F})q^{1/2}d(q-1) > 0$ for sufficiently large q. By taking $\mathcal{F}$ to be the set $\mathcal{F}_b$, and $l_i = 0$ for all $1 \le i \le M$, the above argument implies that for sufficiently large m, subject to condition 2, a primitive polynomial $p(x)$ exists of degree m such that $a(f) \equiv 0 \pmod h$ for all $f \in \mathcal{F}_b$, where $f(x) \equiv x^{a(f)} \pmod{p(x)}$. From Theorem 3, such $p(x)$ satisfies the AES conditions associated with $e(x)$, and, by Theorem 2, the polynomial $e(x)p(x)$ generates an optimum cyclic b-burst-correcting code. So we have proved the following theorem.

Theorem 4: Let $e(x)$ be a square-free polynomial of degree $b-1$ which is not divisible by x. Then, for all sufficiently large $m \equiv 0 \pmod{m_e}$, where m_e is the degree of the splitting field of $e(x)$, a primitive polynomial $p(x)$ of degree m exists such that $e(x)p(x)$ generates an optimum b-burst-correcting code of length $2^m - 1$.

IV. Three-Burst-Correcting Codes

For $b = 3$, the only polynomial $e(x)$ which satisfies condition 1 is $1 + x + x^2$. Hence the generator polynomial of a cyclic three-burst-correcting code has the form $(1 + x + x^2)p(x)$, where $p(x)$ is a primitive polynomial of even degree $m \ge 4$ which satisfies the AES conditions associated with $1 + x + x^2$. It can be verified that these conditions reduce to one condition, namely, $a(1 + x) \not\equiv 2 \pmod 3$. Abramson [1] found primitive polynomials which satisfy this condition for $m = 4, 6, 8, 10$, and he conjectured that they exist for all even $m \ge 4$. Elspas and Short [4] found all primitive polynomials of degree m which satisfy the same condition for $m = 4, 6, 8, 10, 12$.

In this section, we prove the Abramson conjecture. First, we state and prove the following lemma.

Lemma 6: Let $m \ge 4$ be an even integer, and suppose that every primitive element α in F_q, $q = 2^m$, satisfies $a \equiv 2 \pmod 3$, where $1 + \alpha = \alpha^a$. Then $\phi(q-1)/(q-1) < 1/3$.

Proof: Let $n = q - 1$, and let $Q_n(x)$ be the nth cyclotomic polynomial. From the hypotheses, every primitive element in F_q satisfies $1 + x = x^a$ for some $a \equiv 2 \pmod 3$. Raising this equation to the $n/3$rd power, we find that every primitive element in F_q satisfies $(1 + x)^{n/3} = x^{2n/3}$, which implies

$$Q_n(x) | (1 + x)^{n/3} + x^{2n/3}. \tag{4.1}$$

On the other hand, $Q_n(x) | (1 + x^n)$, and $(1 + x^n) = (1 + x^{n/3})(1 + x^{n/3} + x^{2n/3})$. Since $\gcd(Q_n(x), 1 + x^{n/3}) =$

1, it follows that

$$Q_n(x) | 1 + x^{n/3} + x^{2n/3}. \tag{4.2}$$

From (4.1) and (4.2), it follows that

$$Q_n(x) | (1 + x)^{n/3} + 1 + x^{n/3}. \tag{4.3}$$

However, $(1 + x)^{n/3} + 1 + x^{n/3} \neq 0$ for $n > 3$, i.e., $m > 2$. Since $\deg Q_n(x) = \phi(n)$, and $\deg((1 + x)^{n/3} + 1 + x^{n/3}) < n/3$, (4.3) implies $\phi(n) < n/3$. ∎

In the following, m is an even number, $m \geq 4$, and $q = 2^m$. Let $\mathcal{F} = \{1 + x\}$ and $l_1 = 2$ in Lemma 4. Then $\sum_{\alpha \in F_q^*} \theta(\alpha)/3$ gives the number of primitive elements α in F_q such that $a \equiv 2 \pmod 3$, where $1 + \alpha = \alpha^a$. If every primitive element in F_q satisfies this condition, then $\sum_{\alpha \in F_q^*} \theta(\alpha)/3 = \phi(q - 1)$. In that case, Lemma 5 implies $\phi(q - 1) \leq q^{1/2} d(q - 1)$, since $A(h, \mathcal{F}) = 2$. The following lemma, which is proved in Appendix II, gives a condition on $q - 1$ which satisfies this inequality.

Lemma 7: If $\phi(q - 1) \leq q^{1/2} d(q - 1)$, then $q - 1$ has at most four distinct prime factors.

However, if $q - 1$ has at most four distinct prime factors, then $\phi(q - 1)/(q - 1) \geq (1 - 1/3)(1 - 1/5)(1 - 1/7)(1 - 1/11) > 1/3$. Lemma 6 then implies the existence of a primitive root α such that $a \not\equiv 2 \pmod 3$, where $1 + \alpha = \alpha^a$. The minimal polynomial of such a primitive element over F_2 is a primitive polynomial $p(x)$ of degree m which satisfies $a \not\equiv 2 \pmod 3$, where $1 + x \equiv x^a \pmod{p(x)}$. Since such a polynomial satisfies the AES condition associated with $1 + x + x^2$, we have proved the following result.

Theorem 5: For every even $m \geq 4$, there exists an optimum cyclic three-burst-correcting code of length $2^m - 1$.

V. Four-Burst-Correcting Codes

For $b = 4$, three polynomials exist that satisfy condition 1, namely, $1 + x^3, 1 + x + x^3$, and $1 + x^2 + x^3$. If $e(x)p(x)$ generates a four-burst-correcting code, then so does $x^r e(x^{-1})p(x^{-1})$, where $r = \deg(e(x)p(x))$. Since $1 + x^2 + x^3 = x^{-3}(1 + x + x^3)$, we may consider only optimum codes generated by $(1 + x^3)p(x)$ and $(1 + x + x^3)p(x)$. In this section, we will be concerned with optimum four-burst-correcting codes generated by $(1 + x^3)p(x)$. Condition 2 implies that $p(x)$ is a primitive polynomial of even degree $m \geq 6$. Elspas and Short [4] found that such codes do not exist for $m < 10$ and showed that they exist for $m = 10, 12$. In this section, we will prove that such codes exist for all even $m \geq 10$.

In the following, we let m denote an even integer, $m \geq 6$, and $q = 2^m$. The AES conditions associated with $1 + x^3$ are deduced in the example of Section II. Note that $a(1 + x) \equiv a(1 + x + x^3) \equiv a(1 + x^2 + x^3) \equiv 0 \pmod 3$ is a solution of these conditions. We define $\mathcal{F} = \{1 + x, 1 + x + x^3, 1 + x^2 + x^3\}$ and look for a primitive element α in F_q which satisfies $a \equiv 0 \pmod 3$, where $f(\alpha) = \alpha^a$, for every $f \in \mathcal{F}$. From Lemmas 4 and 5, it follows that such a primitive element exists if $\phi(q - 1) > A(h, \mathcal{F}) q^{1/2} d(q - 1)$, where $A(h, \mathcal{F}) = 126$ in our case. The minimal polynomial of such a primitive element is a primitive polynomial of degree m which satisfies the AES conditions associated with $1 + x^3$. The following lemma is proved in Appendix II.

Lemma 8: If $q = 2^m$ for some even $m \geq 26$, then $\phi(q - 1) > 126 q^{1/2} d(q - 1)$.

From this lemma, it follows that optimum cyclic four-burst-correcting codes, whose generator polynomials have the form $(1 + x^3)p(x)$, exist for all even $m \geq 26$, where $m = \deg p(x)$. For every even m, $10 \leq m \leq 24$, we found, by computer search, a primitive polynomial $p(x)$ of degree m which satisfies the AES conditions. These polynomials are exhibited in Table I, where $p(x) = \sum_{i=0}^{m} p_i x^i$ is represented by listing the i's for which $p_i = 1$. Thus the following theorem is proved.

TABLE I
Primitive Polynomials Satisfying the AES Conditions Associated with $1 + x^3$

m	$p(x)$
10	(0235, 10)
12	(0125789, 11, 12)
14	(0168, 14)
16	(07, 10, 12, 13, 14, 16)
18	(0245689, 10, 11, 12, 18)
20	(02347, 10, 14, 17, 20)
22	(0159, 22)
24	(012348, 11, 12, 13, 16, 18, 19, 20, 22, 24)

Theorem 6: For every even $m \geq 10$ there exists an optimum cyclic four-burst-correcting code of length $2^m - 1$.

In case of optimum four-burst-correcting codes generated by $(1 + x + x^3)p(x)$, and in general optimum b-burst-correcting codes generated by $e(x)p(x)$, the same procedure can be used to determine the possible lengths of such codes. First, we find the AES conditions associated with $e(x)$. Then we use Lemma 5, along with Lemmas 14 and 15 in Appendix II, to find a number m^* such that for all $m \geq m^*$ and subject to condition 2 optimum b-burst-correcting codes of length $2^m - 1$ exist. For $m < m^*$, a computer search can be used to look for a primitive polynomial $p(x)$ of degree m which satisfies the AES conditions. Unfortunately, the complexity of this technique becomes very large even for moderate values of b.

VI. Five-Burst-Correcting Codes

Elspas and Short [4] reported that no optimum cyclic five-burst-correcting code exists with a length 4095 or less. From Theorem 4, we know that such codes exist for sufficiently large lengths. In this section, we will give the generator polynomial of an optimum five-burst-correcting code of length $2^{15} - 1$.

For $b = 5$, the polynomial $e(x) = (1 + x)(1 + x + x^3) = 1 + x^2 + x^3 + x^4$ satisfies Condition 1. From Theorem 2, the polynomial $(1 + x^2 + x^3 + x^4)p(x)$ generates an optimum five-burst-correcting code if and only if $p(x)$ is a primitive polynomial of degree m such that $3 | m$, $m \geq 6$,

and $p(x)$ satisfies the AES conditions associated with $1 + x^2 + x^3 + x^4$, which consist of the following 28 incongruences modulo 7:

1) $a_1 \not\equiv 3$,
2) $a_2 \not\equiv 5$
3) $a_1 + 6a_2 \not\equiv 5$
4) $a_1 + 3a_2 \not\equiv 4$
5) $a_1 + 2a_2 \not\equiv 6$
6) $a_1 + 6a_3 \not\equiv 6$
7) $a_1 + 3a_3 \not\equiv 1$
8) $a_1 + 2a_3 \not\equiv 4$
9) $a_1 + a_2 \not\equiv 1$
10) $a_1 + a_2 + 6a_3 \not\equiv 4$
11) $a_3 \not\equiv 4$
12) $a_2 + 6a_3 \not\equiv 1$
13) $a_4 \not\equiv 6$
14) $a_2 + 6a_4 \not\equiv 6$
15) $a_3 + 6a_4 \not\equiv 5$
16) $a_2 + 3a_3 \not\equiv 3$
17) $a_2 + 3a_4 \not\equiv 2$
18) $a_5 \not\equiv 2$.
19) $a_2 + 6a_5 \not\equiv 3$
20) $a_3 + 6a_5 \not\equiv 2$
21) $a_4 + 6a_5 \not\equiv 4$
22) $a_2 + 3a_5 \not\equiv 4$
23) $a_6 \not\equiv 1$
24) $a_2 + 6a_6 \not\equiv 4$
25) $a_3 + 6a_6 \not\equiv 3$
26) $a_4 + 6a_6 \not\equiv 5$
27) $a_2 + 3a_6 \not\equiv 1$
28) $a_5 + 6a_6 \not\equiv 1$

where $a_1 = a(1 + x)$, $a_2 = a(1 + x + x^2)$, $a_3 = a(1 + x^2 + x^3)$, $a_4 = a(1 + x + x^4)$, $a_5 = a(1 + x^3 + x^4)$, and $a_6 = a(1 + x + x^2 + x^3 + x^4)$.

We looked for a primitive polynomial of degree 15 that satisfies these conditions. Lemma 5 does not guarantee the existence of such polynomial. Fortunately, we found that the polynomial $1 + x + x^2 + x^3 + x^5 + x^9 + x^{10} + x^{13} + x^{15}$ does satisfy the AES conditions associated with $1 + x^2 + x^3 + x^4$. Hence the polynomial $(1 + x^2 + x^3 + x^4)(1 + x + x^2 + x^3 + x^5 + x^9 + x^{10} + x^{13} + x^{15})$ generates an optimum five-burst-correcting code of length $2^{15} - 1$.

Appendix I
Proof of Theorem 1

Let $g(x)$ be the generator polynomial of an optimum cyclic b-burst-correcting code of length $2^m - 1$. Then deg $g(x) = m + b - 1$, and $g(x) | x^{2^m-1} + 1$. This implies that $g(x)$ is a square-free polynomial which is not divisible by x. Write $g(x) = f_1(x) \cdots f_k(x)$ for some k where the polynomials $f_i(x)$, $1 \le i \le k$ are distinct irreducible polynomials. Let r_i and h_i denote the degree and the period of $f_i(x)$, respectively. Then $\sum_{i=1}^{k} r_i = m + b - 1$. Since $f_i(x) | x^{2^m-1} + 1$, it follows that $r_i | m$, which implies $r_i \le m$ for $1 \le i \le k$. Since $g(x)$ must have period $2^m - 1$, which is the code length, then $2^m - 1 = \text{LCM}(h_1, \cdots, h_k)$. Since $h_i | 2^{r_i} - 1$, it follows that

$$2^m - 1 | \text{LCM}(2^{r_1} - 1, \cdots, 2^{r_k} - 1). \tag{A.1}$$

From a result in [13], it follows that if $m \neq 6$, then a prime π exists such that $\pi | 2^m - 1$ and $\pi \nmid 2^{m'} - 1$ for all $m' < m$. Thus (A.1) implies that if $m \neq 6$, then $r_j = m$ for some j, where $1 \le j \le k$. The same conclusion holds for $m = 6$, since if $r_i < m$ and $r_i | m$ for all $1 \le i \le k$, then LCM $(2^{r_1} - 1, \cdots, 2^{r_k} - 1) | (2^2 - 1)(2^3 - 1) = 21 < 2^6 - 1$, contradicting (A.1). Thus $r_j = m$ for some j, $1 \le j \le k$. Such j is unique, since if it is not, then $m + b - 1 = \sum_{i=1}^{k} r_i \ge 2m$, which contradicts the Rieger bound $m \ge b + 1$. Without loss of generality, let $j = 1$. Next, we prove that $h_1 = 2^m - 1$. We have $(x^{h_1} + 1)g(x)/f_1(x) \equiv 0 \pmod{g(x)}$. Since $\deg(g(x)/f_1(x)) = b - 1$, the code is not a b-burst-correcting code unless $h_1 = 2^m - 1$. Thus $f_1(x)$ is a primitive polynomial of degree m. We take $p(x) = f_1(x)$ and $e(x) = g(x)/f_1(x)$ to get Theorem 1. ■

Appendix II

In this Appendix, we will prove Lemmas 7 and 8. First, we study the arithmetical function $\eta(n) = \phi(n)/(d(n)n^{1/2})$ for odd values of n. The function $\eta(n)$ is multiplicative. If p is a prime and c is a positive integer, then

$$\eta(p^c) = \frac{p^{c/2}(1 - 1/p)}{c + 1}. \tag{A.2}$$

The following four lemmas can be deduced easily from (A.2).

Lemma 9: If $1 \le c_1 \le c_2$, where c_1 and c_2 are integers, and if p is an odd prime, then $\eta(p^{c_1}) \le \eta(p^{c_2})$.

Lemma 10: If c is a nonnegative integer, and p_1 and p_2 are primes with $p_1 \le p_2$, then $\eta(p_1^c) \le \eta(p_2^c)$.

Lemma 11: If c is a nonnegative integer and p is a prime, then $\eta(p)^c \le \eta(p^c)$.

Lemma 12: For $p = 3$ or 5, $\eta(p) < 1$, and for any prime $p \ge 7$, we have $\eta(p) > 1$.

In the following lemma, we define π_i to be the ith odd prime, so that $\pi_1 = 3$, $\pi_2 = 5, \cdots$, etc.

Lemma 13: Let $A \ge 1$ and suppose that $\eta(n) < A$ for some odd n. Then, n has at most k distinct prime factors, where k is the smallest positive integer such that $\prod_{i=1}^{k+1} \eta(\pi_i) \ge A$.

Proof: Write $n = p_1^{c_1} \cdots p_r^{c_r}$, where the p_i's are distinct odd primes, $p_i < p_{i+1}$ for $1 \le i < r$, and the c_i's are positive integers. From Lemma 9 and the fact that η is multiplicative, we have $\prod_{i=1}^{r} \eta(p_i) \le \prod_{i=1}^{r} \eta(p_i^{c_i}) = \eta(n) < A$. From the definition of π_i it follows that $\pi_i \le p_i$ for $1 \le i \le r$. Lemma 10 then gives $\prod_{i=1}^{r} \eta(\pi_i) \le \prod_{i=1}^{r} \eta(p_i) < A$. Since $A \ge 1$, Lemma 12 and the definition of k imply that $k \ge 2$. If $r > k$, then by Lemma 12 we have $\prod_{i=1}^{r} \eta(\pi_i) \ge \prod_{i=1}^{k+1} \eta(\pi_i)$. Hence $\prod_{i=1}^{k+1} \eta(\pi_i) < A$, which contradicts the definition of k. ■

Proof of Lemma 7: Suppose that $q - 1$ has more than four distinct prime factors. Then $q - 1 > 3 \times 5 \times 7 = 105$. However, $q^{1/2} < 1.01(q - 1)^{1/2}$ for $q > 105$. Hence we have $\phi(q - 1) < 1.01(q - 1)^{1/2} d(q - 1)$, i.e., $\eta(q - 1) < 1.01$. By applying Lemma 13, we get a contradiction to the assumption that $q - 1$ has more than four distinct prime factors. ■

Now we proceed to prove Lemma 8. We need an upper bound on n, where n is odd and satisfies $\eta(n) < A$ for a given $A > 0$.

Lemma 14: If $\eta(n) < A$ for some odd integer $n = p_1^{c_1} \cdots p_r^{c_r}$, and $A > 0$, then $c_1 + \cdots + c_r \le K$, where K is the smallest

positive integer such that

$$\frac{3^{(K+1)/2}}{K+2} \geq 8A.$$

Proof: We relabel the p's, if necessary, so that $p_i < p_{i+1}$. From the definition of π_i, we have $\pi_i \leq p_i$ for $1 \leq i \leq r$. Hence from Lemma 10,

$$\prod_{i=1}^{r} \eta(\pi_i^{c_i}) \leq \sum_{i=1}^{r} \eta(p_i^{c_i}) = \eta(n) < A. \qquad \text{(A.3)}$$

If $\pi_i \geq 17$, then $(\pi_i/3)^{c/2}(1 - \pi_i^{-1})/(c+1) \geq (16/17)(17/3)^{c/2}(c+1)^{-1} > 1$. Hence $\eta(\pi_i^c) > 3^{c/2}$. By using a similar argument, one can prove that $1.1\eta(13^c) > 3^{c/2}$, $1.2\pi(11^c) > 3^{c/2}$, $1.6\eta(7^c) > 3^{c/2}$, and $2.5\eta(5^c) > 3^{c/2}$. Hence

$$(1.1)(1.2)(1.6)(2.5)\prod_{i=1}^{r} \eta(\pi_i^{c_i}) \geq \frac{3^{(c_1+\cdots+c_r)/2}}{c_1+1}(1-1/3) \geq \frac{2}{3}\frac{3^{(c_1+\cdots+c_r)/2}}{c_1+\cdots+c_r+1}.$$

From (A.3), we get

$$\frac{3^{(c_1+\cdots+c_r)/2}}{c_1+\cdots+c_r+1} \leq \frac{3}{2}(1.1)(1.2)(1.6)(2.5)A < 8A.$$

Since $3^{a/2}/(a+1)$, for integer $a \geq 1$, is an increasing function of a, it follows from the definition of K that $c_1 + \cdots + c_r \leq K$. ■

Lemma 15: Let A be a positive number. Define, for $i \geq 1$, q_i to be the smallest prime, $q_i \geq 7$, that satisfies $\eta(3)\eta(5)\eta^i(\bar{q}_i) \geq A$, where $\bar{q}_i$ denotes the smallest prime larger than q_i. Then, $\eta(n) < A$ for odd n implies that $n \leq \Pi_{i=1}^{K} q_i$ where K is defined in Lemma 14.

Proof: Write $n = p_1^{c_1} \cdots p_r^{c_r}$, where $p_i > p_{i+1}$ for $1 \leq i \leq r$. From Lemmas 9–12 we have

$$\eta(n) = \prod_{i=1}^{r} \eta(p_i^{c_i}) \geq \prod_{i=1}^{r} \eta(p_i)^{c_i} \geq \eta(3)\eta(5)\prod_{i=1}^{j} \eta(p_i)^{c_i} \geq \eta(3)\eta(5)\eta(p_j)^{c_1+\cdots+c_j}$$

where $1 \leq j \leq r$. Hence $\eta(3)\eta(5)\eta(p_j)^{c_1+\cdots+c_j} < A$. From the definition of q_i, it follows that $p_j \leq q_{c_1+\cdots+c_j}$. Hence $p_1^{c_1}p_2^{c_2} \cdots p_r^{c_r} \leq q_{c_1}^{c_1} q_{c_1+c_2}^{c_2} \cdots q_{c_1+\cdots+c_r}^{c_r}$. Since $q_i \geq 7$, then from Lemma 12, as well as the definition of q_i, it follows that $q_i \geq q_{i+1}$. Hence $n = p_1^{c_1} \cdots p_r^{c_r} \leq \Pi_{i=1}^{c_1+\cdots+c_r} q_i \leq \Pi_{i=1}^{K} q_i$ by Lemma 14. ■

Proof of Lemma 8: Suppose that $\phi(q-1) \leq 126q^{1/2}d(q-1)$. Since $m \geq 26$, we have $q^{1/2} < 1.0001(q-1)^{1/2}$, and $\phi(q-1) \leq 126.1(q-1)^{1/2}d(q-1)$, i.e., $\eta(q-1) \leq 126.1$. We apply Lemma 14 with $A = 126.1$ to get $K = 17$. We then apply Lemma 15 to get $q < 2^{89}$. Next, we check $\eta(q-1)$, where $q = 2^m$ for every even m, $26 \leq m \leq 88$. This can be done by looking at tables for the factorization of $2^m - 1$, e.g., [14]. We find that $\eta(q-1) > 126.1$ for all such values of m, which contradicts the assumption we started with. This proves Lemma 8. ■

References

[1] N. M. Abramson, "Error-correcting codes from linear sequential circuits," presented at the 4th Symp. on Information Theory, London, England, Aug. 29–Sept. 2, 1960.

[2] S. H. Rieger, "Codes for the correction of clustered errors," *IRE Trans. Inform. Theory*, vol. IT-6, pp. 16–21, Mar. 1960.

[3] N. M. Abramson, "A class of systematic codes for non-independent errors," *IRE Trans. Inform. Theory*, vol. IT-5, pp. 150–157, Dec. 1959.

[4] B. Elspas and R. A. Short, "A note on optimum burst-error-correcting codes," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 39–42, Jan. 1962.

[5] R. W. Lucky, J. Salz, and E. J. Weldon, Jr., *Principles of Data Communications*. New York: McGraw-Hill, 1968.

[6] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed. Cambridge, MA: MIT Press, 1971.

[7] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, NJ: Prentice-Hall, 1979.

[8] R. E. Blahut, *Theory and Practice of Error Control Codes*. Reading, MA: Addison-Wesley, 1983.

[9] R. Lidl and H. Niederreiter, *Finite Fields*, Reading, MA: Addison-Wesley, 1983.

[10] W. M. Schmidt, *Equations over Finite Fields*, Lecture Notes in Math., vol. 539, New York: Springer-Verlag, 1976.

[11] L. Carlitz, "Primitive roots in a finite field," *Trans. Amer. Math. Soc.*, vol. 73, pp. 373–382, 1952.

[12] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed. Oxford: Oxford Univ. Press, 1983.

[13] L. E. Dickson, "On the cyclotomic function," *Amer. Math. Mon.*, vol. 12, pp. 86–89, 1905.

[14] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckermam, and S. S. Wagstaff, Jr., *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to High Powers*, Contemporary Mathematics, vol. 22. Amer. Math. Soc., 1982.